KENTUCKY

DEPARTMENT OF INSURANCE

GUIDE TO

FEDERAL PRIVACY

REQUIREMENTS

June 20, 2001

TABLE OF CONTENTS

Glossary of Terms:

The following terms are used throughout this document:

"Affiliate" is a company that controls, is controlled by, or is under common control with another company. Under the Gramm-Leach-Bliley Act (GLBA), insurers and banks can become affiliates. Affiliates may be parent companies, companies owned by your company or agency, or common companies under the same holding company structure.

"Consumers" are individuals who are seeking to obtain, obtaining, or have obtained a product or service from an insurer. For example, an individual who has submitted an application for insurance is a consumer of the company to which he or she has applied, as is an individual whose policy with the company has expired. A consumer can also be a prospect seeking an insurance product, or a beneficiary or claimant under an insurance policy.

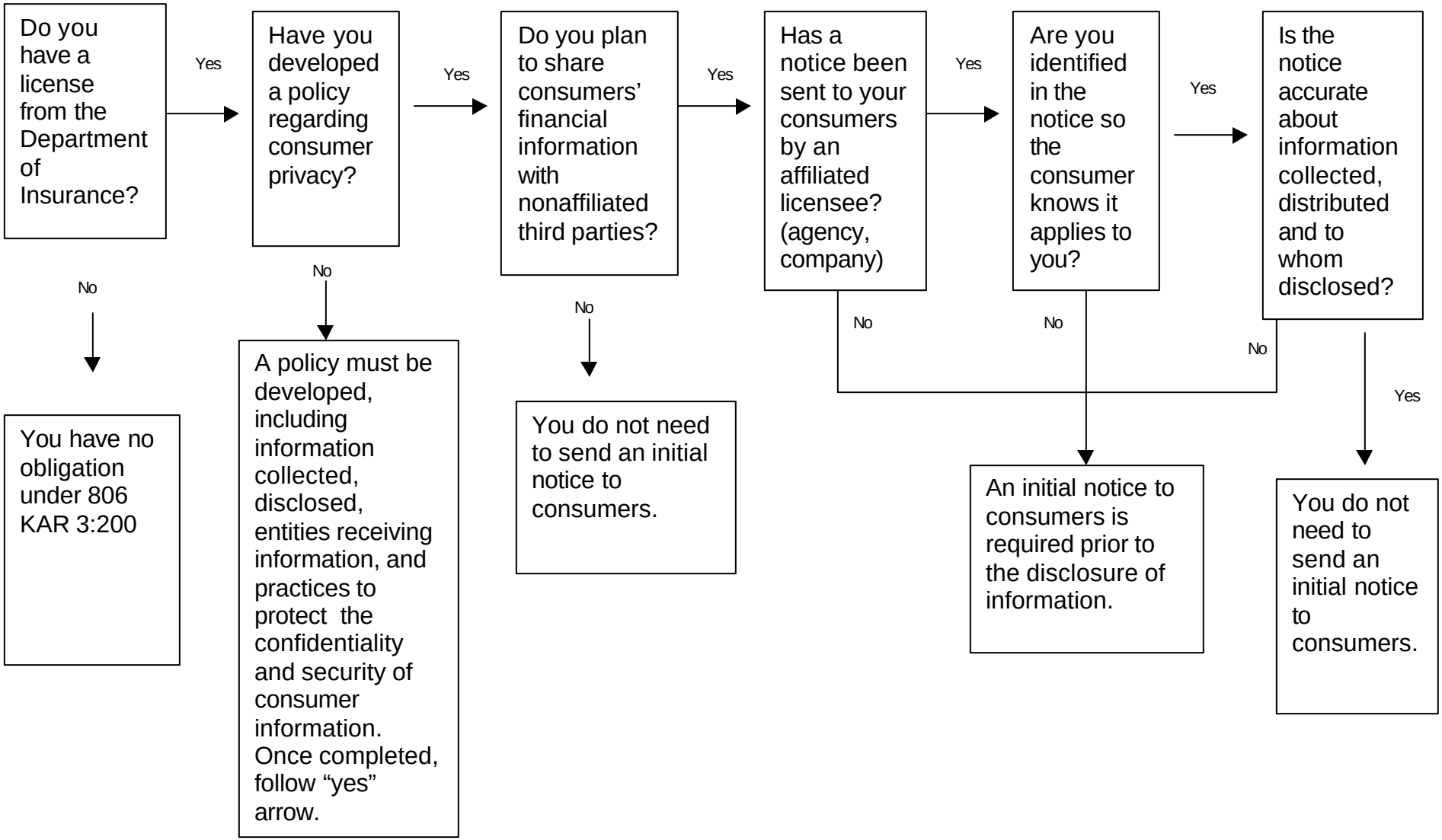
"Customers" are consumers with whom insurers have on-going relationships. Policyholders and investment clients are customers, for example.

"Insurers" are insurance companies, insurance agents, or other entities that are required to comply with the privacy regulation.

"Licensees" are all individuals regulated by the Department of Insurance. All licensees are required to comply with 806 KAR 3:200 according to the federal Gramm-Leach-Bliley Act.

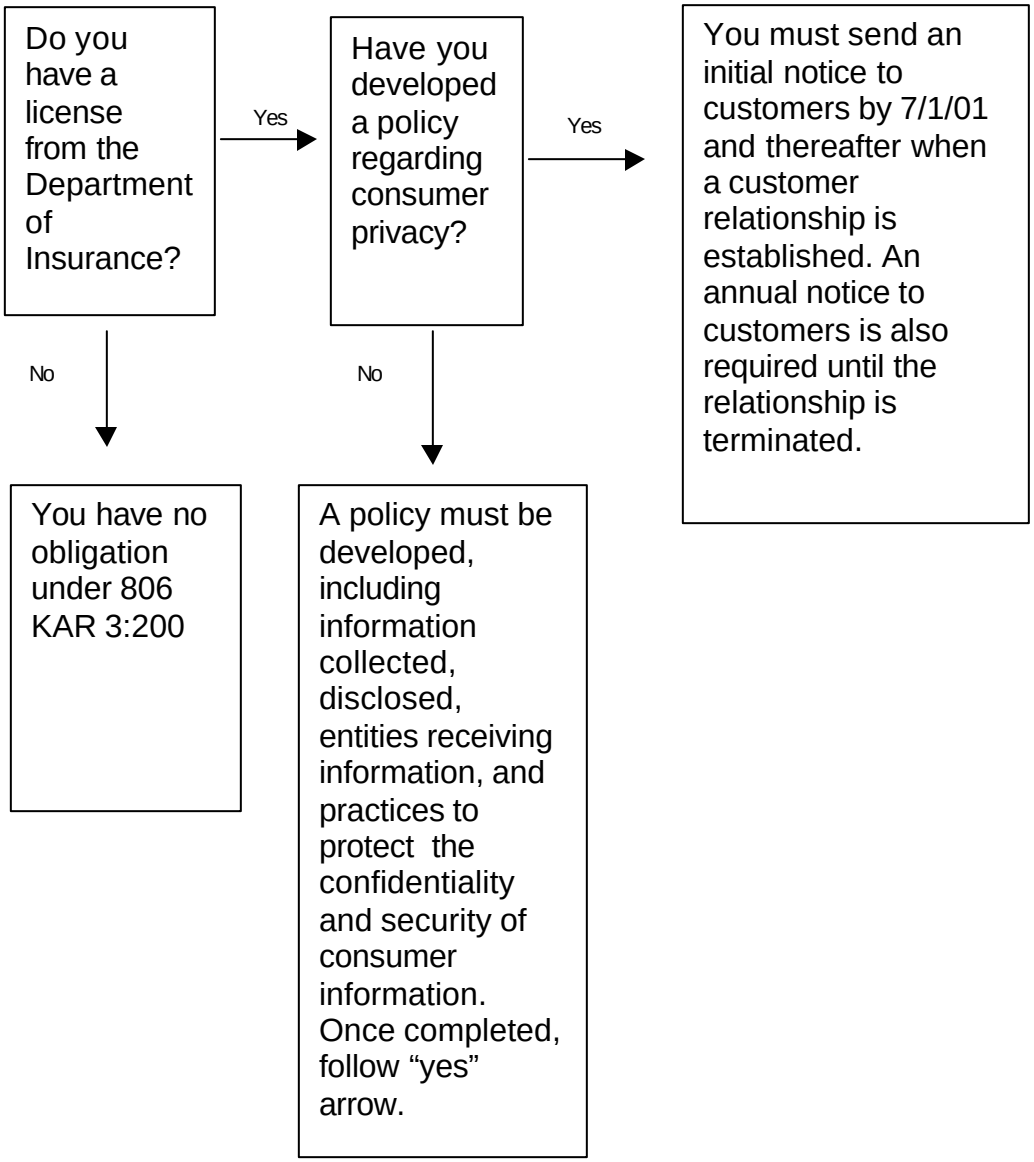
"Nonaffiliated third party" means a company that is not affiliated with an insurer, agent or agency.

WHAT ARE YOUR OBLIGATIONS FOR HANDLING CONSUMERS' FINANCIAL INFORMATION



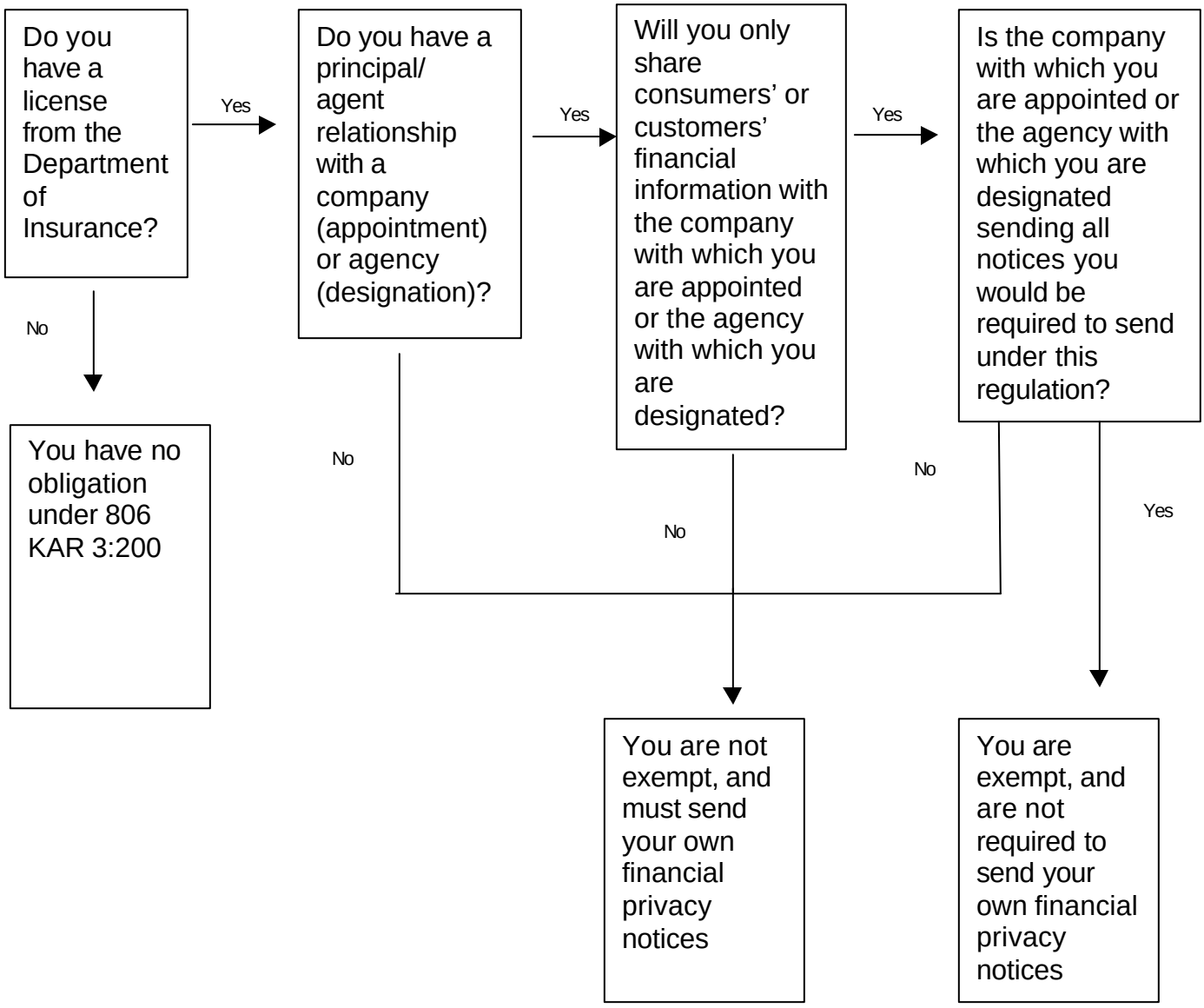
This information is provided as a courtesy of the Kentucky Department of Insurance. The responsibility to understand and comply with 806 KAR 3:210 and 806 KAR 3:220 remains with the licensee.

WHAT ARE YOUR OBLIGATIONS FOR HANDLING CUSTOMERS' FINANCIAL INFORMATION



This information is provided as a courtesy of the Kentucky Department of Insurance. The responsibility to understand and comply with 806 KAR 3:210 and 806 KAR 3:220 remains with the licensee.

ARE YOU EXEMPT?
(FINANCIAL INFORMATION ONLY)



This information is provided as a courtesy of the Kentucky Department of Insurance. The responsibility to understand and comply with 806 KAR 3:210 and 806 KAR 3:220 remains with the licensee.

General Rules for Financial Information:

➢ Consumers:

- A licensee may not disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice unless a revised notice is provided.

- A revised notice must contain a description of privacy policies and practices, a new opt-out notice, and a reasonable time to opt-out prior to the disclosure of information.

- A licensee may not disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party, unless:

    - The consumer received a notice prior to disclosure
    - The consumer received an explanation of the opt-out procedure
    - The consumer had a reasonable opportunity to opt-out prior to disclosure, and
    - The consumer did not opt-out

➢ Customers:

- A customer must be given an annual notice of the licensee's privacy policies and practices until such time as the customer relationship terminates.

- A licensee may not disclose any nonpublic personal information about a customer to a nonaffiliated third party other than as described in the initial notice unless a revised notice is provided.

- A revised notice must contain a description of privacy policies and practices, a new opt-out notice, and a reasonable time to opt-out prior to the disclosure of information.

- A licensee may not disclose any nonpublic personal financial information about a customer to a nonaffiliated third party, unless:

    - The customer received an initial notice
    - The customer received an explanation of the opt-out procedure
    - The customer had a reasonable opportunity to opt-out prior to disclosure, and
    - The customer did not opt-out

Information to be included in Privacy Notices:

Initial, annual and revised notices must include:

- Categories of nonpublic personal financial information collected
- Categories of nonpublic personal financial information disclosed
- Categories of affiliates and nonaffiliated third parties to whom information is disclosed, except as part of an insurance transaction
- Categories of nonpublic personal financial information about former customers disclosed and to whom disclosed
- Categories of information disclosed and to whom disclosed as a result of contractual relationships for servicing or joint marketing
- Explanation of consumers' right to opt-out of disclosure of his nonpublic personal financial information to nonaffiliated third parties and the methods to utilize to opt-out
- Any disclosures made according to the federal Fair Credit Reporting Act, Section 603(d)(2)(A)(iii) of 15 U.S.C. 1681a(d)(2)(A)(iii)
- Policies and practices for protecting the confidentiality and security of nonpublic personal financial information
- If making disclosures as part of an insurance transaction, that the licensee makes disclosures to other affiliated or nonaffiliated third parties, as permitted by law.

Simplified Notices:

If you do not disclose nonpublic financial information about customers, and you do not wish to reserve the right to disclose nonpublic financial information about customers or former customers, your notice may simply state that fact and provide the following information:

- The categories of nonpublic personal financial information that you collect;
- Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and
- A statement that the disclosures made to affiliated or non-affiliated third parties are permitted by law.

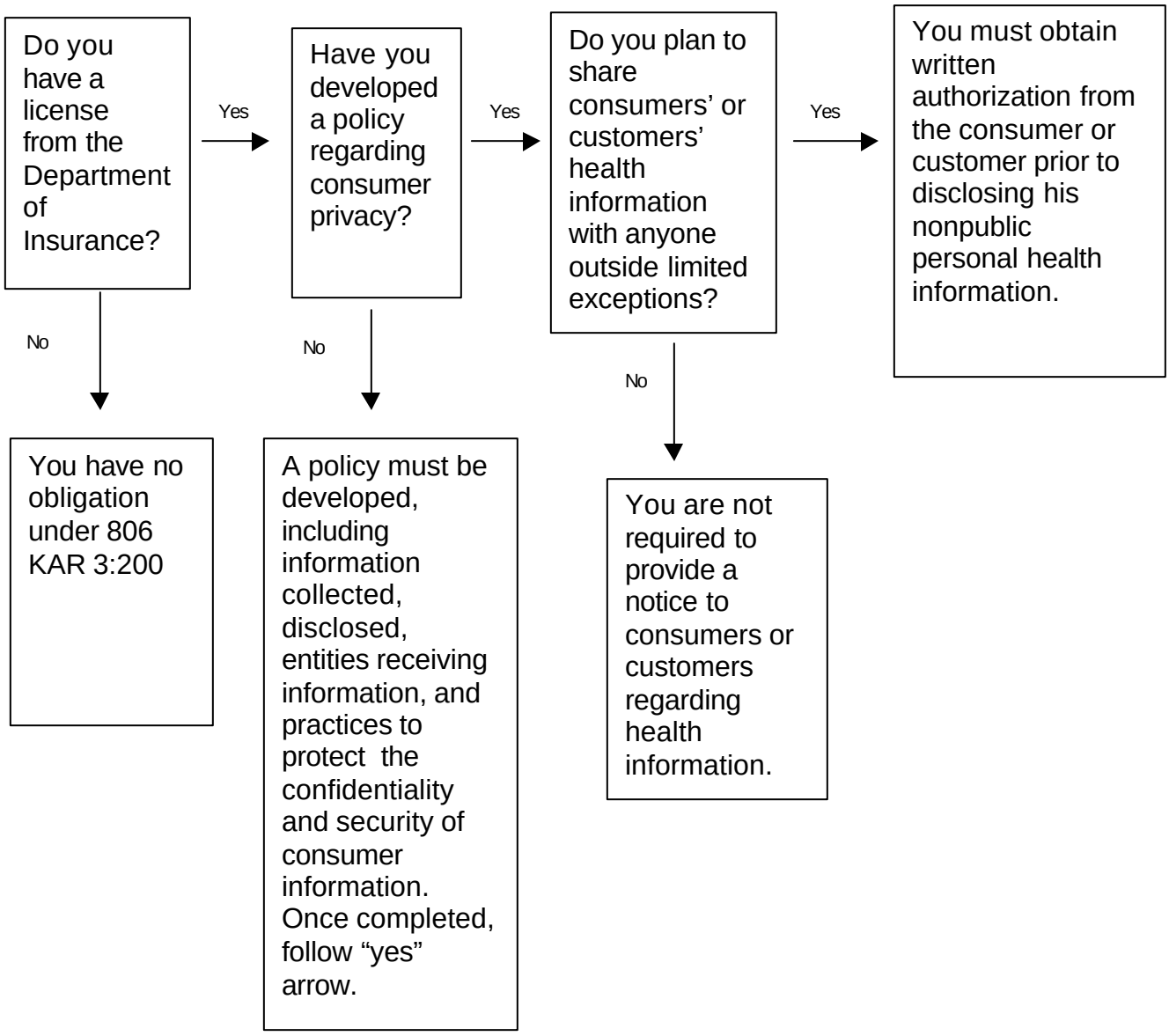
This information is provided as a courtesy of the Kentucky Department of Insurance. The responsibility to understand and comply with 806 KAR 3:210 and 806 KAR 3:220 remains with the licensee.

Opt-out Notices:

Notice must be clear and conspicuous and include:

- The licensee discloses or reserves the right to disclose nonpublic personal financial information about the consumer or customer to a nonaffiliated third party;
- The consumer or customer has a right to opt-out of that disclosure; and
- A reasonable means for the consumer or customer to exercise the right to opt-out.

WHAT ARE YOUR OBLIGATIONS FOR HANDLING CONSUMERS' AND CUSTOMERS' HEALTH INFORMATION



This information is provided as a courtesy of the Kentucky Department of Insurance. The responsibility to understand and comply with 806 KAR 3:210 and 806 KAR 3:220 remains with the licensee.

General Rules for Health Information:

➢ Consumers and Customers

- A licensee may not disclose the nonpublic personal health information of a consumer or customer to an affiliate or a non-affiliated third party unless an authorization is given from the individual whose information is sought to be disclosed.

- An authorization to disclose nonpublic personal health information must include:
  - The identity of the consumer or customer;
  - A description of the type of information to be disclosed;
  - General descriptions of parties receiving the information;
  - The consumer's or customer's signature;
  - The length of time the authorization is valid and the procedure for revoking the authorization.

FREQUENTLY ASKED QUESTIONS:

1. Who is required to comply with the privacy regulations?

With some limited exceptions, all companies, agents and other persons and entities licensed under Kentucky's insurance laws are required to comply with the regulation, including health insurers and HMOs, which are considered "financial institutions" under the Gramm-Leach-Bliley Act.

2. I'm a surplus lines broker. Does the privacy regulation apply to me?

Yes, the regulation does apply to surplus lines brokers. However, you are not required to comply with the financial information notice and opt out provisions if:

- you do not disclose any nonpublic personal information for any purpose including joint marketing and servicing, (except that you may disclose information pursuant to the specific business and legal exceptions); and

- you deliver a notice to your consumers and customers stating that fact.

3. Are third party administrators (TPAs) or managing general agents (MGAs) subject to the regulation?

All entities that are licensed under Kentucky's insurance laws are required to comply with the privacy regulations, including all licensed TPAs and MGAs.

4. Are workers' compensation plans covered by the regulation?

Yes, workers' compensation plans are subject to the regulation, although they are treated slightly differently from other insurers:

- **Financial Information:** A workers' compensation plan is only required to provide privacy and opt out notices to a person who receives benefits from the plan (a "beneficiary") if the plan wishes to disclose the beneficiary's nonpublic personal financial information to a third party outside the extensive exceptions provided in the regulation. In such a situation, the beneficiary is the plan's "consumer." Workers' compensation plans are also required to provide annual privacy notices to all plan participants.

- **Health Information:** Workers' compensation plans must comply with the same health privacy protections that apply to other insurers. Therefore, a workers' compensation plan must get the permission of a beneficiary before sharing that person's nonpublic personal health information (except when information is shared pursuant to one or more of the exceptions set out in the regulation).

5. Does the privacy regulation specifically apply to agents?

Yes, the privacy regulations does apply to agents. However, an agent does not have to comply with the notice and opt out requirements of the regulation if:

- the agent is appointed with a company or designated with an agency (a "principal") that complies with, and provides all of the notices required by the regulation; and

- the agent does not disclose protected information to any person other than the principal or its affiliates.

So, if an agent wishes to disclose a consumer's protected information to an entity other than the insurance company with which the agent is appointed or the agency with which the agent is designated, the agent must give the consumer a copy of the agent's privacy notice and an opportunity to prohibit the disclosure of that information to non-affiliated third parties.

6. I'm a paid representative of one insurance company and I only represent that company and its line of insurance and financial services products. What are my responsibilities under this new privacy rule?

You are subject to the regulation, but you are not required to comply with the notice and opt out requirements of the regulation if:

- the company with which you are appointed complies with the regulation; and

- you do not disclose protected information to any person other than that company or its affiliates.

7. I'm an independent agent and therefore represent a variety of insurance companies. What are my responsibilities under the privacy rule?

Just like other agents, you are subject to the regulation, but you are not required to comply with the notice and opt out requirements of the regulation if:

- the company (or companies) for which you are appointed or the agency with which you are designated, with respect to a particular consumer or customer complies with the regulation; and

- you do not disclose protected information to any person other than that company (or companies), agency or the affiliates of that company or agency.

8. I am a licensed insurance agent and I sell variable annuities. Am I required to comply with the privacy rule?

Yes, you are subject to the privacy regulations. However, just like other agents, you are not required to comply with the notice and opt out requirements of the regulation if:

- the company for which you are appointed or the agency for which you are designated with respect to a particular consumer or customer complies with the regulation; and

- you do not disclose protected information to any person other than that company, agency or the affiliates of that company or agency.

9. I'm an independent agent and need to share consumer information with many insurers in order to get the best prices for my clients. Is this permissible under the privacy regulation?

Yes, an agent may share protected information with multiple companies in an effort to compare prices, at the consumer's request. In such situations, the individual will be a consumer of each of the companies and will be entitled to privacy and opt out notices from any of the companies that wishes to share the individual's protected financial information with non-affiliated third parties. The individual's consent will be required prior to disclosure of protected health information.

Note that at the time of purchase, these individuals are considered to be your customers.

10. Do I have to go back to every one of my existing clients and tell them about this new rule?

Not necessarily. You are required to provide privacy and opt out notices by July 1, 2001, to a client if the client is your "customer." A client is considered your customer if he or she obtains financial, investment or economic advisory services relating to an insurance product or service from you for a fee, or if the individual obtains insurance through you.

If you are appointed with a company or designated with an agency (a "principal"), however, you are not required to provide privacy notices to your customer if:

- the principal complies with the regulation with respect to that customer; and
- you do not disclose protected information about that customer to any person other than the principal or its affiliates.

If you are required to send privacy and opt out notices to existing clients, they must be sent by July 1, 2001, which is the compliance date set forth in the regulation.

It is important to note that starting on the compliance date, all new clients will be either consumers or customers, and will be entitled to the privacy and opt out notices required by the regulation.

11. Every company is different. Of the companies I represent, how am I supposed to know which ones sent out notices?

Like all aspects of the agent-agency or agent-company relationship, effective compliance with privacy regulations will require on-going communication and coordination between the parties.

12. What if one of my clients didn't receive a notice from a company? Who is responsible?

Specific compliance issues will be decided on a case-by-case basis, of course. However, it is the responsibility of the agent to determine whether the company's or agency's notice is sufficient to exempt the agent from providing his independent notice. If the agent provides a notice to the client, he or she would have a good argument that he or she should not be held responsible for the company's omission.

13. Our agency receives phone-in requests for information on the insurance products offered by the companies we represent. Do we have to tell these callers the privacy policy of each of the companies when they call in?

Not necessarily. If these individuals are simply requesting information and not purchasing a product, they are likely to be considered consumers – either your consumers or consumers of the companies for which you are acting as agent, or both. If you collect protected personal information about these individuals and you are going to share that information with non-affiliated third parties, you will be required to provide them privacy and opt out notices prior to disclosure of any protected personal information. On the other hand, if you are not going to disclose any non-public personal information to non-affiliated third parties, you have no obligations to provide privacy and opt out notices to the individual. Finally, if you are going to disclose information only pursuant to a joint marketing or servicing agreement, a privacy notice is all that is required; the consumer is not entitled to opt out.

If an individual actually purchases a product from you over the telephone, that individual is considered a customer. Normally, customers are entitled to privacy and opt out notices at the time the customer relationship is established. With a telephone transaction, however, delivery of notices can be delayed with the customer's consent.

The same obligations would apply to the companies for which you are appointed as agent.

14. I'm an independent agent and I perform servicing and processing functions for several insurers. Does the privacy regulation permit the exchange of information necessary for me to continue to perform these functions?

Yes. An insurer can share nonpublic personal information with agents acting as service providers for a variety of purposes regardless of whether a consumer permits disclosure of his or her information.

Section 14 of the financial privacy regulation specifically permits companies to share nonpublic personal financial information with third parties to enable them to perform services for the company or functions on the company's behalf. The only requirements are (i) the company must provide an initial notice to the individual, and (ii) the company must enter into a written agreement with the third party prohibiting the third party from using the information other than to carry out the purposes for which the information was disclosed and pursuant to the exceptions in the rule.

Section 15 of the financial privacy regulation permits companies to share nonpublic personal financial information with third parties, including agents, for numerous servicing purposes including: servicing or processing an insurance product that a consumer requests or authorizes; carrying out the service business of which the consumer's transaction is a part; and administering or servicing benefits or claims. Such disclosures are subject to the regulation's reuse and redisclosure provisions, which generally prohibit third parties that receive information under an exception from using such information other than to carry out the purposes for which the information was disclosed and pursuant to the exceptions in the rule.

The health privacy regulation permits companies to share nonpublic personal health information with affiliates and third parties, including agents, for numerous insurance activities such as claims administration, fraud reporting, and policy placement and issuance.

15. How does the new regulation impact the disclosure of information about beneficiaries?

- For the treatment of **workers' compensation beneficiaries**, see question 4.

- A **beneficiary of a life insurance policy** is considered a consumer under the regulation if you disclose nonpublic personal financial information about the beneficiary to a nonaffiliated third party outside the exceptions provided in the regulation. As a consumer, such a beneficiary is entitled to a privacy notice and the opportunity to opt out of the disclosure of nonpublic personal financial information.

- A **beneficiary of an employee benefit plan** is considered a consumer if you disclose nonpublic personal financial information about the beneficiary to a nonaffiliated third party outside the exceptions provided in the regulation. As a consumer, such a beneficiary is entitled to a privacy notice and the opportunity to opt out of the disclosure of nonpublic personal financial information. You are also required to provide annual notices to plan sponsors, regardless of whether you disclose beneficiary information to nonaffiliated third parties.

- **Health Information:** You are required to get the consent of beneficiaries prior to disclosing nonpublic personal health information to any other party (except when information is shared pursuant to one or more of the exceptions set out in the regulation).

16. How does the new regulation impact the disclosure of information about claimants?

- **Financial Information:** A claimant under any insurance policy is considered a consumer under the regulation if you disclose nonpublic personal financial information about the claimant to a nonaffiliated third party outside the exceptions provided in the regulation. As a consumer, such a claimant is entitled to a privacy notice and the opportunity to opt out of the disclosure of nonpublic personal financial information.

- **Health Information:** You are required to get the consent of claimants prior to disclosing nonpublic personal health information to any other party (except when information is shared pursuant to one or more of the exceptions set out in the regulation).

17. What if I have nonpublic personal information about a claimant and I do not share it?

You have no obligation to a claimant if you do not share nonpublic personal financial information with third parties or nonpublic personal health information with any other party.

18. What if I have nonpublic personal information about a beneficiary and I do not share it?

You have no obligation to beneficiaries if you do not share their nonpublic personal financial information with third parties or nonpublic personal health information with any other party. However, you are required to provide initial, annual and revised privacy notices to employee benefit plan sponsors, group or blanket insurance policyholders, group annuity contract holders and workers' compensation plan participants (employers).

19. My appointed company provides on-going settlement options for beneficiaries and claimants. If a beneficiary or claimant takes advantage of such an option, is that person a consumer or a customer?

Beneficiaries and claimants that submit a claim under a policy choosing a settlement option involving an on-going relationship with an insurer are considered consumers, not customers. Thus, the company and agent will be required to provide the individuals with privacy notices and an opportunity to opt out if the company wishes to disclose the individual's nonpublic personal information to third parties. Affirmative consent is required for the disclosure

of health information. There are no on-going privacy policy notice requirements.

20. I know I must send privacy notices to customers and certain consumers regarding financial information, but am I required to send notices to customers and consumers if we only have health information about them?

No. The notice provisions of the privacy regulation do not apply to health information. The only time you are required to disclose the types of health information you possess and what you are going to do with that health information is when you contact consumers and customers to ask them to consent to the disclosure of such information.

21. To whom do we have to give annual privacy policy notices?

You are required to provide your customers with annual privacy notices. "Customers" are individuals with whom you have on-going relationships. Policyholders are customers, for example. In contrast, prospects and applicants are consumers and are only entitled to privacy notices if you wish to share their protected financial information with third parties. Similarly, beneficiaries and claimants are only entitled to receive privacy notices if you wish to disclose their protected information with third parties.

22. What happens if I do not get privacy notices to all of our customers by July 1, 2001?

If you have not sent privacy notices to all your customers by July 1, 2001, you will be in violation of the regulation. A violation of the regulation will be considered a violation of the unfair trade practices act. The Kentucky Department of Insurance has many avenues available to enforce such laws. The type of enforcement action will depend upon the severity of the violation.

23. What happens if I forget to give a privacy notice to a consumer?

You are not required to give a privacy notice to a consumer unless you wish to disclose nonpublic personal financial information regarding that consumer to a nonaffiliated third party. So, if you do not give the consumer a notice and do not disclose his or her information to a third party, there is no problem. If, however, you do not give the consumer a notice and you do disclose his or her information to a third party, you would be in violation of the regulation and subject to applicable enforcement actions.

24. Can I send privacy notices, opt out notices and health information authorizations together in the same mailing? Can they be sent with other customer mailings?

Privacy, opt out and health authorization notices can be sent together or separately, and they can be sent with other customer mailings. In addition, affiliated companies may send notices together, or they can send combined notices. No matter how they are sent, however, all notices must identify the companies and policies to which they apply. They must be accurate, and they must be clear and conspicuous so that the customer can read and understand them.

25. If a customer of an agent is at the county clerk's office to renew their license plate and the county clerk calls the agent to get proof of insurance because the customer did not bring it with them, and asks him to fax it to the clerk's office so the agent's customer can complete his license transaction, would the agent be able to do this under the exception in Section 15 of the proposed regulation 806 KAR 3:200?

Yes, a notice and opportunity to opt-out of the sharing of the consumer's information would not be necessary, as the agent is sharing the information at the consumer's request.

26. If a customer's policy is subject to renewal, may an agent request quotes from various insurance companies in an effort to shop the coverage without providing notice to the customer and an opportunity to opt-out?

Yes, if the customer has requested the shopping of his or her insurance coverage. If the customer has not requested the renewal quotes, his information cannot be shared with companies unless a privacy notice was provided to him and the customer did not opt-out of the disclosure.

27. Are utilization review entities, assessment companies and health discount plans subject to the privacy regulations?

Yes, all entities and persons regulated by the Kentucky Department of Insurance are considered "licensees" for purposes of the financial privacy regulation and the health privacy regulation. An entity is regulated by the Department of Insurance if it has a license, certificate of authority, certificate of filing, certificate of registration or similar authorization to engage in the business of insurance issued by the Department.

28. May an agent share financial information with a non-affiliated premium finance company without providing notice to the consumer?

Yes, sharing application information with a premium finance company is an exception to the notice and opt-out requirements under Section 15 of the financial privacy regulation as a disclosure "necessary to effect, administer or enforce a transaction." However, should the consumer elect to purchase the insurance product, he becomes a customer and must receive notice at that time.

29. Are companies or agents required to provide notice and the opportunity to opt-out prior to disclosing a customer's financial or health information to the Department of Insurance?

No, sharing information with regulatory authorities having jurisdiction over the company or agent is an exempt disclosure under the regulations.

30. May the privacy notice issued by an insurance company include appointed agencies and designated agents?

If a company is sending all privacy notices that would otherwise be required to be sent by its appointed agent, the company notice identifies the appointed agent and the agent agrees not to disclose any information about consumers or customers to any person or entity other than the company, the company's notice may include the appointed agent. However, if an agency is appointed with the company and the agent is only designated with the agency, the company's notice cannot include the designated agent. For further information, please refer to the flowchart on page 5, entitled "Are you exempt?"